Drahtlose Sensornetze in der Lehre – Sicherheitsbetrachtung von ZigBee-Netzen

Björn Stelte
Institut für Technische Informatik
Universität der Bundeswehr München
bjoern.stelte@unibw.de

Gerade in den letzten Jahren kommen mehr und mehr Anwendungen auf Basis von drahtlosen Sensornetze auf dem Markt. So gibt es in den USA die Bestrebungen drahtlose Sensornetze für die Energieüberwachung (smart monitoring) einzusetzen, aber auch in der Hausautomatisierung, dem Gesundheitswesen, u.a. sind die Netze bestehend aus vielen kleinen Sensorknoten im Gespräch. Der de-facto Standard bzgl. der Kommunikation dieser Sensornetze ist derzeit ZigBee. Dieses Protokoll wird in nahezu allen gängigen Sensornetzen verwendet. Jedoch sind bereits seit einiger Zeit Schwächen dieses Protokolls bekannt. Wie Joshua Wright mit seinem KillerBee Framework gezeigt hat, ist ein praktischer Angriff auf eine ZigBee Infrastruktur mit wenigen Hilfsmitteln kostengünstig und schnell realisierbar. Dieser Beitrag gibt einen Überblick über das ZigBee Protokoll und einige seiner Schwachstellen, sowie über Werkzeuge, um die Problematik im Unterricht darzustellen.

In der Lehre ist es häufig erforderlich zum einen aktuelle und spannende Themen aufzugreifen aber zum anderen auch diese den Studenten geeignet zu vermitteln. Eine Demonstration von Kommunikationsabläufen sicherheitskritischer Datenkommunikation und insbesondere die Erklärung der Funktionsweise von Angriffen auf selbige anhand einer Simulation erhöht den Lerneffekt. Die in diesem Beitrag aufgezeigte Sicherheits-Problematik des ZigBee Protokolls ist ein aktuelles Thema. Die vorgeschlagenen Simulationen können bspw. im Unterricht oder bei Beteiligung der Studenten in einem Praktikum verwendet werden, um die Aspekte der IT-Sicherheit dem Studenten nahezubringen. Wir haben die Erfahrung gesammelt, dass der Drei-Satz Erkennen, Analysieren, Absichern den besten Lerneffekt erzielt. So sind die drei vorgestellten Simulationen in genau dieser Reihung zu sehen. Die erste Simulation schult das Erkennen der Problematik, die zweite Simulation vermittelt eine Analyse des Angriffs (hier KillerBee) und letztendlich wird in der dritten Simulation die Absicherung des Netzes anhand eines Beispiels erlernt. Weitere Angriffe auf ZigBee Netze sind möglich, so kann bei Interesse die Simulationsaufgabe nach belieben noch erweitert oder ausgebaut werden.

Der vollständige Beitrag kann unter der Adresse `http://inf3-www.informatik.unibw-muenchen.de/ZigBee_sec_lehre.pdf` abgerufen werden.